

The automorphism group of a self-dual [72, 36, 16] code does not contain \mathcal{S}_3 , \mathcal{A}_4 and D_8

Martino Borello*, Francesca Dalla Volta[†] and Gabriele Nebe^{‡ §}

March 21, 2013

Abstract

A computer calculation with MAGMA shows that there is no extremal self-dual binary code \mathcal{C} of length 72, whose automorphism group contains the symmetric group of degree 3, the alternating group of degree 4 or the dihedral group of order 8. Combining this with the known results in the literature one obtains that $\text{Aut}(\mathcal{C})$ has order ≤ 5 or isomorphic to the elementary abelian group of order 8.

1 Introduction

Let $\mathcal{C} = \mathcal{C}^\perp \leq \mathbb{F}_2^n$ be a binary *self-dual* code of length n . Then the weight $\text{wt}(c) := |\{i \mid c_i = 1\}|$ of every $c \in \mathcal{C}$ is even. When in particular $\text{wt}(\mathcal{C}) := \{\text{wt}(c) \mid c \in \mathcal{C}\} \subseteq 4\mathbb{Z}$, the code is called *doubly-even*. Using invariant theory, one may show [10] that the minimum weight $d(\mathcal{C}) := \min(\text{wt}(\mathcal{C} \setminus \{0\}))$ of a doubly-even self-dual code is bounded from above by $4 + 4 \lfloor \frac{n}{24} \rfloor$. Self-dual codes achieving this bound are called *extremal*. Extremal self-dual codes of length a multiple of 24 are particularly interesting for various reasons: for example they are always doubly-even [12] and all their codewords of a given nontrivial weight support 5-designs [2]. There are unique extremal self-dual codes of length 24 (the extended binary Golay code \mathcal{G}_{24}) and 48 (the extended quadratic residue code QR_{48}) and both have a fairly big automorphism group (namely $\text{Aut}(\mathcal{G}_{24}) \cong M_{24}$ and $\text{Aut}(QR_{48}) \cong \text{PSL}_2(47)$). The existence of an extremal code of length 72 is a long-standing open problem [13]. A series of papers investigates the automorphism group of a putative extremal self-dual code of length

*M. Borello is with the Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano Bicocca, 20125 Milan, Italy, e-mail: m.borello1@campus.unimib.it.

[†]F. Dalla Volta is with the Dipartimento di Matematica e Applicazioni, Università degli Studi di Milano Bicocca, 20125 Milan, Italy, e-mail: francesca.dallavolta@unimib.it.

[‡]G. Nebe is with the Lehrstuhl D für Mathematik, RWTH Aachen University, 52056 Aachen, Germany, e-mail: nebe@math.rwth-aachen.de.

[§]Borello and Dalla Volta are members of INdAM-GNSAGA, Italy. Dalla Volta and Nebe have been partially supported by MIUR-Italy via PRIN “Group theory and applications”

72 excluding most of the subgroups of \mathcal{S}_{72} . The most recent result is contained in [3] where the first author excluded the existence of automorphisms of order 6.

In this paper we prove that neither \mathcal{S}_3 nor \mathcal{A}_4 nor D_8 is contained in the automorphism group of such a code.

The method to exclude \mathcal{S}_3 (which is isomorphic to the dihedral group of order 6) is similar to the one used for the dihedral group of order 10 in [8] and based on the classification of additive trace-Hermitian self-dual codes in \mathbb{F}_4^{12} obtained in [7].

For the alternating group \mathcal{A}_4 of degree 4 and the dihedral group D_8 of order 8 we use their structure as a semidirect product of an elementary abelian group of order 4 and a group of order 3 and 2 respectively. By [11] we know that the fixed code of any element of order 2 is isomorphic to a self-dual binary code D of length 36 with minimum distance 8. These codes have been classified in [1]; up to equivalence there are 41 such codes D . For all possible lifts $\tilde{D} \leq \mathbb{F}_2^{72}$ that respect the given actions we compute the codes $\mathcal{E} := \tilde{D}^{\mathcal{A}_4}$ and $\mathcal{E} := \tilde{D}^{D_8}$ respectively. We have respectively only three and four such codes \mathcal{E} with minimum distance ≥ 16 . Running through all doubly-even \mathcal{A}_4 -invariant self-dual overcodes of \mathcal{E} we see that no such code is extremal. Since the group D_8 contains a cyclic group of order 4, say C_4 , we use the fact [11] that \mathcal{C} is a free $\mathbb{F}_2 C_4$ -module. Checking all doubly-even self-dual overcodes of \mathcal{E} which are free $\mathbb{F}_2 C_4$ -modules we see that, also in this case, there is none extremal.

The present state of research is summarized in the following theorem.

Theorem 1.1. *The automorphism group of a self-dual [72, 36, 16] code is either cyclic of order 1, 2, 3, 4, 5 or elementary abelian of order 4 or 8.*

All results are obtained using extensive computations in MAGMA [4].

2 The symmetric group of degree 3.

2.1 Preliminaries

Let \mathcal{C} be a binary self-dual code and let g be an automorphism of \mathcal{C} of odd prime order p . Define $\mathcal{C}(g) := \{c \in \mathcal{C} \mid c^g = c\}$ and $\mathcal{E}(g)$ the set of all the codewords that have even weight on the cycles of g . From a module theoretical point of view, \mathcal{C} is a $\mathbb{F}_2\langle g \rangle$ -module and $\mathcal{C}(g) = \mathcal{C} \cdot (1 + g + \dots + g^{p-1})$ and $\mathcal{E}(g) = \mathcal{C} \cdot (g + \dots + g^{p-1})$.

In [9] Huffman notes (it is a special case of Maschke's theorem) that

$$\mathcal{C} = \mathcal{C}(g) \oplus \mathcal{E}(g).$$

In particular it is easy to prove that the dimension of $\mathcal{E}(g)$ is $\frac{(p-1) \cdot c}{2}$ where c is the number of cycles of g .

In a usual manner we can identify vectors of length p with polynomials in $\mathcal{Q} := \mathbb{F}_2[x]/(x^p - 1)$; that is (v_1, v_2, \dots, v_p) corresponds to $v_1 + v_2 x + \dots + v_p x^{p-1}$. The weight of a polynomial is the number of nonzero coefficients. Let $\mathcal{P} \subset \mathcal{Q}$

be the set of all the even weight polynomials. If $1 + x + \dots + x^{p-1}$ is irreducible in $\mathbb{F}_2[x]$ then \mathcal{P} is a field with identity $x + x^2 + \dots + x^{p-1}$ [9]. There is a natural map, that we will describe only in our particular case in the next section, from $\mathcal{E}(g)$ to \mathcal{P}^c . Let us observe here only the fact that, if $p = 3$, $1 + x + x^2$ is irreducible in $\mathbb{F}_2[x]$ and \mathcal{P} is isomorphic to \mathbb{F}_4 , the field with four elements. The identification is the following:

0	000	ω	110
1	011	$\overline{\omega}$	101

2.2 The computations for \mathcal{S}_3

Let \mathcal{C} be an extremal self-dual code of length 72 and suppose that $G \leq \text{Aut}(\mathcal{C})$ with $G \cong \mathcal{S}_3$. Let σ denote an element of order 2 and g an element of order 3 in G . By [6] and [5] we have that σ and g have no fixed points. So, in particular, σ has 36 2-cycles and g has 24 3-cycles. Let us suppose, w.l.o.g. that

$$\sigma = (1, 4)(2, 6)(3, 5) \dots (67, 70)(68, 72)(69, 71)$$

and

$$g = (1, 2, 3)(4, 5, 6) \dots (67, 68, 69)(70, 71, 72).$$

As we have seen in Section 2.1, we have

$$\mathcal{C} = \mathcal{C}(g) \oplus \mathcal{E}(g)$$

where $\mathcal{E}(g)$ is the subcode of \mathcal{C} of all the codewords with an even weight on the cycles of g , of dimension 24. We can consider a map

$$f : \mathcal{E}(g) \rightarrow \mathbb{F}_4^{24}$$

extending the identification $\mathcal{P} \cong \mathbb{F}_4$, stated in Section 2.1, to each cycle of g .

Again by [9], we have that $\mathcal{E}(g)' := f(\mathcal{E}(g))$ is an Hermitian self-dual code over \mathbb{F}_4 (that is $\mathcal{E}(g)' = \left\{ \epsilon \in \mathbb{F}_4^{24} \mid \sum_{i=0}^{24} \epsilon_i \overline{\gamma_i} = 0 \text{ for all } \gamma \in \mathcal{E}(g)' \right\}$, where $\overline{\alpha} = \alpha^2$ is the conjugate of α in \mathbb{F}_4). Clearly the minimum distance of $\mathcal{E}(g)'$ is ≥ 8 . So $\mathcal{E}(g)'$ is a $[24, 12, \geq 8]_4$ Hermitian self-dual code.

The action of σ on the $\mathcal{C} \leq \mathbb{F}_2^{72}$ induces an action on $\mathcal{E}(g)' \leq \mathbb{F}_4^{24}$, namely

$$(\epsilon_1, \epsilon_2, \dots, \epsilon_{23}, \epsilon_{24})^\sigma = (\overline{\epsilon_2}, \overline{\epsilon_1}, \dots, \overline{\epsilon_{24}}, \overline{\epsilon_{23}})$$

Note that this action is only \mathbb{F}_2 -linear. In particular, the subcode fixed by σ , say $\mathcal{E}(g)'(\sigma)$, is

$$\mathcal{E}(g)'(\sigma) = \{(\epsilon_1, \overline{\epsilon_1}, \dots, \epsilon_{12}, \overline{\epsilon_{12}}) \in \mathcal{E}(g)'\}$$

Proposition 2.1. (cf. [8, Cor. 5.6]) *The code*

$$\mathcal{X} := \pi(\mathcal{E}(g)'(\sigma)) := \{(\epsilon_1, \dots, \epsilon_{12}) \in \mathbb{F}_4^{12} \mid (\epsilon_1, \overline{\epsilon_1}, \dots, \epsilon_{12}, \overline{\epsilon_{12}}) \in \mathcal{E}(g)'\}$$

is an additive trace-Hermitian self-dual $(12, 2^{12}, \geq 4)_4$ code such that

$$\mathcal{E}(g)' := \phi(\mathcal{X}) := \langle (\epsilon_1, \overline{\epsilon_1}, \dots, \epsilon_{12}, \overline{\epsilon_{12}}) \mid (\epsilon_1, \dots, \epsilon_{12}) \in \mathcal{X} \rangle_{\mathbb{F}_4}.$$

Proof. For $\gamma, \epsilon \in \mathcal{X}$ the inner product of their preimages in $\mathcal{E}(g)'(\sigma)$ is

$$\sum_{i=1}^{12} (\epsilon_i \overline{\gamma_i} + \overline{\epsilon_i} \gamma_i)$$

which is 0 since $\mathcal{E}(g)'(\sigma)$ is self-orthogonal. Therefore \mathcal{X} is trace-Hermitian self-orthogonal. The dimension

$$\dim_{\mathbb{F}_2}(\mathcal{X}) = \dim_{\mathbb{F}_2}(\mathcal{E}(g)'(\sigma)) = \frac{1}{2} \dim_{\mathbb{F}_2}(\mathcal{E}(g)')$$

since $\mathcal{E}(g)'$ is a projective $\mathbb{F}_2\langle\sigma\rangle$ -module, and so \mathcal{X} is self-dual. Since $\dim_{\mathbb{F}_2}(\mathcal{X}) = 12 = \dim_{\mathbb{F}_4}(\mathcal{E}(g)'),$ the \mathbb{F}_4 -linear code $\mathcal{E}(g)' \leq \mathbb{F}_4^{24}$ is obtained from \mathcal{X} as stated. \square

All additive trace-Hermitian self-dual codes in \mathbb{F}_4^{12} are classified in [7]. There are 195,520 such codes that have minimum distance ≥ 4 , up to monomial equivalence.

Remark 2.2. Notice that if \mathcal{X} and \mathcal{Y} are monomial equivalent, via a 12×12 monomial matrix $M := (m_{i,j})$, then $\phi(\mathcal{X})$ and $\phi(\mathcal{Y})$ are monomial equivalent too, via the 24×24 monomial matrix $M' := (m'_{i,j})$, where $m'_{2i-1,2j-1} = m_{i,j}$ and $m'_{2i,2j} = \overline{m_{i,j}}$, for all $i, j \in \{1, \dots, 12\}$.

An exhaustive search with MAGMA gives that the minimum distance of $\phi(\mathcal{X})$ is ≤ 6 , for each of the 195,520 additive trace-Hermitian self-dual $(12, 2^{12}, \geq 4)_4$ codes. But $\mathcal{E}(g)'$ should have minimum distance ≥ 8 , a contradiction. So we proved the following.

Theorem 2.3. *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain a subgroup isomorphic to S_3 .*

3 The alternating group of degree 4 and the dihedral group of order 8.

3.1 The action of the Klein four group.

For the alternating group \mathcal{A}_4 of degree 4 and the dihedral group D_8 of order 8 we use their structure

$$\begin{aligned} \mathcal{A}_4 &\cong \mathcal{V}_4 : C_3 \cong (C_2 \times C_2) : C_3 = \langle g, h \rangle : \langle \sigma \rangle \\ D_8 &\cong \mathcal{V}_4 : C_2 \cong (C_2 \times C_2) : C_2 = \langle g, h \rangle : \langle \sigma \rangle \end{aligned}$$

as a semidirect product.

Let \mathcal{C} be some extremal $[72, 36, 16]$ code such that $\mathcal{H} \leq \text{Aut}(\mathcal{C})$ where $\mathcal{H} \cong \mathcal{A}_4$ or $\mathcal{H} \cong D_8$. Then by [6] and [5] all non trivial elements in \mathcal{H} act without fixed

points and we may replace \mathcal{C} by some equivalent code so that

$$\begin{aligned} g &= (1, 2)(3, 4)(5, 6)(7, 8)(9, 10)(11, 12) \dots (71, 72) \\ h &= (1, 3)(2, 4)(5, 7)(6, 8)(9, 11)(10, 12) \dots (70, 72) \\ \sigma &= (1, 5, 9)(2, 7, 12)(3, 8, 10)(4, 6, 11) \dots (64, 66, 71) \quad (\text{for } \mathcal{A}_4) \\ \sigma &= (1, 5)(2, 8)(3, 7)(4, 6) \dots (68, 70) \quad (\text{for } D_8) \end{aligned}$$

Let

$$\mathcal{G} := C_{\mathcal{S}_{72}}(\mathcal{H}) := \{t \in \mathcal{S}_{72} \mid tg = gt, th = ht, t\sigma = \sigma t\}$$

denote the centralizer of this subgroup \mathcal{H} in \mathcal{S}_{72} . Then \mathcal{G} acts on the set of extremal \mathcal{H} -invariant self-dual codes and we aim to find a system of orbit representatives for this action.

Definition 3.1. *Let*

$$\begin{aligned} \pi_1 : \{v \in \mathbb{F}_2^{72} \mid v^g = v\} &\rightarrow \mathbb{F}_2^{36} \\ (v_1, v_1, v_2, v_2, \dots, v_{36}, v_{36}) &\mapsto (v_1, v_2, \dots, v_{36}) \end{aligned}$$

denote the bijection between the fixed space of g and \mathbb{F}_2^{36} and

$$\begin{aligned} \pi_2 : \{v \in \mathbb{F}_2^{72} \mid v^g = v \text{ and } v^h = v\} &\rightarrow \mathbb{F}_2^{18} \\ (v_1, v_1, v_1, v_1, v_2, \dots, v_{18}) &\mapsto (v_1, v_2, \dots, v_{18}) \end{aligned}$$

the bijection between the fixed space of $\langle g, h \rangle \trianglelefteq \mathcal{A}_4$ and \mathbb{F}_2^{18} . Then h acts on the image of π_1 as

$$\pi_1(h) = (1, 2)(3, 4) \dots (35, 36).$$

Let

$$\begin{aligned} \pi_3 : \{v \in \mathbb{F}_2^{36} \mid v^{\pi_1(h)} = v\} &\rightarrow \mathbb{F}_2^{18}, \\ (v_1, v_1, v_2, v_2, \dots, v_{18}, v_{18}) &\mapsto (v_1, v_2, \dots, v_{18}), \end{aligned}$$

so that $\pi_2 = \pi_3 \circ \pi_1$.

Remark 3.2. *The centraliser $C_{\mathcal{S}_{72}}(g) \cong C_2 \wr \mathcal{S}_{36}$ of g acts on the set of fixed points of g . Using the isomorphism π_1 we hence obtain a group epimorphism which we again denote by π_1*

$$\pi_1 : C_{\mathcal{S}_{72}}(g) \rightarrow \mathcal{S}_{36}$$

with kernel C_2^{36} . Similarly we obtain the epimorphism

$$\pi_3 : C_{\mathcal{S}_{36}}(\pi_1(h)) \rightarrow \mathcal{S}_{18}.$$

The normalizer $N_{\mathcal{S}_{72}}(\langle g, h \rangle)$ acts on the set of $\langle g, h \rangle$ -orbits which defines a homomorphism

$$\pi_2 : N_{\mathcal{S}_{72}}(\langle g, h \rangle) \rightarrow \mathcal{S}_{18}.$$

Let us consider the fixed code $\mathcal{C}(g)$ which is isomorphic to

$$\pi_1(\mathcal{C}(g)) = \{(c_1, c_2, \dots, c_{36}) \mid (c_1, c_1, c_2, c_2, \dots, c_{36}, c_{36}) \in \mathcal{C}\}.$$

By [11], the code $\pi_1(\mathcal{C}(g))$ is some self-dual code of length 36 and minimum distance 8. These codes have been classified in [1], up to equivalence (under the action of the full symmetric group \mathcal{S}_{36}) there are 41 such codes. Let

$$Y_1, \dots, Y_{41}$$

be a system of representatives of these extremal self-dual codes of length 36.

Remark 3.3. $\mathcal{C}(g) \in \mathcal{D}$ where

$$\mathcal{D} := \left\{ D \leq \mathbb{F}_2^{36} \mid \begin{array}{l} D = D^\perp, d(D) = 8, \pi_1(h) \in \text{Aut}(D) \\ \text{and } \pi_2(\sigma) \in \text{Aut}(\pi_3(D(\pi_1(h)))) \end{array} \right\}.$$

For $1 \leq k \leq 41$ let $\mathcal{D}_k := \{D \in \mathcal{D} \mid D \cong Y_k\}$.

Let $\mathcal{G}_{36} := \{\tau \in C_{\mathcal{S}_{36}}(\pi_1(h)) \mid \pi_3(\tau)\pi_2(\sigma) = \pi_2(\sigma)\pi_3(\tau)\}$.

Remark 3.4. For $\mathcal{H} \cong \mathcal{A}_4$ the group \mathcal{G}_{36} is isomorphic to $C_2 \wr C_3 \wr \mathcal{S}_6$. It contains $\pi_1(\mathcal{G}) \cong \mathcal{A}_4 \wr \mathcal{S}_6$ of index 64.

For $\mathcal{H} \cong D_8$ we get $\mathcal{G}_{36} = \mathcal{G} \cong C_2 \wr C_2 \wr \mathcal{S}_9$.

Lemma 3.5. A set of representatives of the \mathcal{G}_{36} orbits on \mathcal{D}_k can be computed by performing the following computations:

- Let h_1, \dots, h_s represent the conjugacy classes of fixed point free elements of order 2 in $\text{Aut}(Y_k)$.
- Compute elements $\tau_1, \dots, \tau_s \in \mathcal{S}_{36}$ such that $\tau_i^{-1}h_i\tau_i = \pi_1(h)$ and put $D_i := Y_k^{\tau_i}$ so that $\pi_1(h) \in \text{Aut}(D_i)$.
- For all D_i let $\sigma_1, \dots, \sigma_{t_i}$ a set of representatives of the action by conjugation by the subgroup $\pi_3(C_{\text{Aut}(D_i)}(\pi_1(h)))$ on fixed point free elements of order 3 (for $\mathcal{H} \cong \mathcal{A}_4$) respectively 2 (for $\mathcal{H} \cong D_8$) in $\text{Aut}(\pi_3(D_i(\pi_1(h))))$.
- Compute elements $\rho_1, \dots, \rho_{t_i} \in \mathcal{S}_{18}$ such that $\rho_j^{-1}\sigma_j\rho_j = \pi_3(\sigma)$, lift ρ_j naturally to a permutation $\tilde{\rho}_j \in \mathcal{S}_{36}$ commuting with $\pi_1(h)$ (defined by $\tilde{\rho}_j(2a-1) = 2\rho_j(a)-1$, $\tilde{\rho}_j(2a) = 2\rho_j(a)$) and put

$$D_{i,j} := (D_i)^{\tilde{\rho}_j} = D^{\tau_i\tilde{\rho}_j}$$

so that $\pi_3(\sigma) \in \text{Aut}(\pi_2(D_{i,j}(\pi_1(h))))$.

Then $\{D_{i,j} \mid 1 \leq i \leq s, 1 \leq j \leq t_i\}$ represent the \mathcal{G}_{36} -orbits on \mathcal{D}_k .

Proof. Clearly these codes lie in \mathcal{D}_k .

Now assume that there is some $\tau \in \mathcal{G}_{36}$ such that

$$Y_k^{\tau_{i'}\tilde{\rho}_{j'}\tau} = D_{i',j'}^\tau = D_{i,j} = Y_k^{\tau_i\tilde{\rho}_j}.$$

Then

$$\epsilon := \tau_{i'} \tilde{\rho}_{j'} \tau \tilde{\rho}_j^{-1} \tau_i^{-1} \in \text{Aut}(Y_k)$$

satisfies $\epsilon h_i \epsilon^{-1} = h_{i'}$, so h_i and $h_{i'}$ are conjugate in $\text{Aut}(Y_k)$, which implies $i = i'$ (and so $\tau_i = \tau_{i'}$). Now,

$$Y_k^{\tau_i \tilde{\rho}_{j'} \tau} = D_i^{\tilde{\rho}_{j'} \tau} = D_i^{\tilde{\rho}_j} = Y_k^{\tau_i \tilde{\rho}_j}.$$

Then

$$\epsilon' := \tilde{\rho}_{j'} \tau \tilde{\rho}_j^{-1} \in \text{Aut}(D_i)$$

commutes with $\pi_1(h)$. We compute that $\pi_3(\epsilon') \sigma_j \pi_3(\epsilon'^{-1}) = \sigma_{j'}$ and hence $j = j'$.

Now let $D \in \mathcal{D}_k$ and choose some $\xi \in \mathcal{S}_{36}$ such that $D^\xi = Y_k$. Then $\pi_1(h)^\xi$ is conjugate to some of the chosen representatives $h_i \in \text{Aut}(Y_k)$ ($i = 1, \dots, s$) and we may multiply ξ by some automorphism of Y_k so that $\pi_1(h)^\xi = h_i = \pi_1(h)^{\tau_i^{-1}}$. So $\xi \tau_i \in C_{\mathcal{S}_{36}}(\pi_1(h))$ and $D^{\xi \tau_i} = Y_k^{\tau_i} = D_i$. Since $\pi_3(\sigma) \in \text{Aut}(\pi_3(D(\pi_1(h))))$ we get

$$\pi_3(\sigma)^{\pi_3(\xi \tau_i)} \in \text{Aut}(\pi_3(D_i(\pi_1(h))))$$

and so there is some automorphism $\alpha \in \pi_3(C_{\text{Aut}(D_i)}(\pi_1(h)))$ and some $j \in \{1, \dots, t_i\}$ such that $(\pi_3(\sigma)^{\pi_3(\xi \tau_i)})^\alpha = \sigma_j$. Then

$$D^{\xi \tau_i \tilde{\alpha} \tilde{\rho}_j} = D_{i,j}$$

where $\xi \tau_i \tilde{\alpha} \tilde{\rho}_j \in \mathcal{G}_{36}$. □

3.2 The computations for \mathcal{A}_4 .

We now deal with the case $\mathcal{H} \cong \mathcal{A}_4$.

Remark 3.6. With MAGMA we use the algorithm given in Lemma 3.5 to compute that there are exactly 25,299 \mathcal{G}_{36} -orbits on \mathcal{D} , represented by, say, $X_1, \dots, X_{25,299}$.

As \mathcal{G} is the centraliser of \mathcal{A}_4 in \mathcal{S}_{72} the image $\pi_1(\mathcal{G})$ commutes with $\pi_1(h)$ and $\pi_2(\mathcal{G})$ centralizes $\pi_2(\sigma)$. In particular the group \mathcal{G}_{36} contains $\pi_1(\mathcal{G})$ as a subgroup. With MAGMA we compute that $[\mathcal{G}_{36} : \pi_1(\mathcal{G})] = 64$. Let $g_1, \dots, g_{64} \in \mathcal{G}_{36}$ be a left transversal of $\pi_1(\mathcal{G})$ in \mathcal{G}_{36} .

Remark 3.7. The set $\{X_i^{g_j} \mid 1 \leq i \leq 25,299, 1 \leq j \leq 64\}$ contains a set of representatives the $\pi_1(\mathcal{G})$ -orbits on \mathcal{D} .

Remark 3.8. For all $1 \leq i \leq 25,299, 1 \leq j \leq 64$ we compute the code

$$\mathcal{E} := E(X_i^{g_j}, \sigma) := \tilde{D} + \tilde{D}^\sigma + \tilde{D}^{\sigma^2}, \text{ where } \tilde{D} = \pi_1^{-1}(X_i^{g_j}).$$

Only for three X_i there are two codes $\tilde{D}_{i,1} = \pi_1^{-1}(X_i^{g_{j_1}})$ and $\tilde{D}_{i,2} = \pi_1^{-1}(X_i^{g_{j_2}})$ such that $E(X_i^{g_{j_1}}, \sigma)$ and $E(X_i^{g_{j_2}}, \sigma)$ are doubly even and of minimum distance

16. In all the three cases, the two codes are equivalent. Let us call the inequivalent codes $\mathcal{E}_1, \mathcal{E}_2$ and \mathcal{E}_3 , respectively. They have dimension 26, 26, and 25, respectively, minimum distance 16 and their automorphism groups are

$$\text{Aut}(\mathcal{E}_1) \cong \mathcal{S}_4, \text{Aut}(\mathcal{E}_2) \text{ of order } 432, \text{Aut}(\mathcal{E}_3) \cong (\mathcal{A}_4 \times \mathcal{A}_5) : 2.$$

All three groups contain a unique conjugacy class of subgroups conjugate in \mathcal{S}_{72} to \mathcal{A}_4 (which is normal for \mathcal{E}_1 and \mathcal{E}_3).

Corollary 3.9. *The code $\mathcal{C}(g) + \mathcal{C}(h) + \mathcal{C}(gh)$ is equivalent under the action of \mathcal{G} to one of the three codes $\mathcal{E}_1, \mathcal{E}_2$ or \mathcal{E}_3 .*

Let \mathcal{E} be one of these three codes. The group \mathcal{A}_4 acts on $\mathcal{V} := \mathcal{E}^\perp / \mathcal{E}$ with kernel $\langle g, h \rangle$. The space \mathcal{V} is hence an $\mathbb{F}_2\langle\sigma\rangle$ -module supporting a σ -invariant form such that \mathcal{C} is a self-dual submodule of \mathcal{V} . As in Section 2.1 we obtain a canonical decomposition

$$\mathcal{V} = \mathcal{V}(\sigma) \perp \mathcal{W}$$

where $\mathcal{V}(\sigma)$ is the fixed space of σ and σ acts as a primitive third root of unity on \mathcal{W} .

For $\mathcal{E} = \mathcal{E}_1$ or $\mathcal{E} = \mathcal{E}_2$ we compute that $\mathcal{V}(\sigma) \cong \mathbb{F}_2^4$ and $\mathcal{W} \cong \mathbb{F}_4^8$. For both codes the full preimage of any self-dual submodule of $\mathcal{V}(\sigma)$ is a code of minimum distance < 16 .

For $\mathcal{E} = \mathcal{E}_3$ the dimension of $\mathcal{V}(\sigma)$ is 2 and there is a unique self-dual submodule of $\mathcal{V}(\sigma)$ so that the full preimage E_3 is doubly-even and of minimum distance ≥ 16 . The element σ acts on $E_3^\perp / E_3 \cong \mathcal{W}$ with irreducible minimal polynomial, so $E_3^\perp / E_3 \cong \mathbb{F}_4^{10}$. The code \mathcal{C} is a preimage of one of the 58,963,707 maximal isotropic \mathbb{F}_4 -subspaces of the Hermitian \mathbb{F}_4 -space E_3^\perp / E_3 . Just for technical reasons it seems to be easier to first compute all 142,855 one dimensional isotropic subspaces $\overline{E}_3 / E_3 \leq_{\mathbb{F}_4} E_3^\perp / E_3$ for which the code \overline{E}_3 has minimum distance ≥ 16 . The automorphism group $\text{Aut}(E_3) = \text{Aut}(\mathcal{E}_3)$ acts on these codes with 1,264 orbits. For all these 1,264 orbit representatives \overline{E}_3 we compute the 114,939 maximal isotropic subspaces of $\overline{E}_3^\perp / \overline{E}_3$ (as the orbits of one given subspace under the unitary group $GU(8, 2)$ in MAGMA) and check whether the corresponding doubly-even self-dual code has minimum distance 16. No such code is found.

This computation hence shows the following main theorem.

Theorem 3.10. *The automorphism group of a self-dual $[72, 36, 16]$ code does not contain a subgroup isomorphic to \mathcal{A}_4 .*

3.3 The computations for D_8 .

For this section we assume that $\mathcal{H} \cong D_8$. Then $\pi_1(\mathcal{G}) = \mathcal{G}_{36}$ and we may use Lemma 3.5 to compute a system of representatives of the $\pi_1(\mathcal{G})$ -orbits on the set \mathcal{D} .

Remark 3.11. $\pi_1(\mathcal{G})$ acts on \mathcal{D} with exactly 9,590 orbits represented by, say, $X_1, \dots, X_{9,590}$. For all $1 \leq i \leq 9,590$ we compute the code

$$\mathcal{E} := E(X_i, \sigma) := \tilde{D} + \tilde{D}^\sigma, \text{ where } \tilde{D} = \pi_1^{-1}(X_i).$$

Only for four X_i the code $E(X_i, \sigma)$ is doubly even and of minimum distance 16. Let us call the inequivalent codes $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ and \mathcal{E}_4 , respectively. They have all dimension 26 and minimum distance 16.

Corollary 3.12. The code $\mathcal{C}(g) + \mathcal{C}(h) + \mathcal{C}(gh)$ is equivalent under the action of \mathcal{G} to one of the four codes $\mathcal{E}_1, \mathcal{E}_2, \mathcal{E}_3$ or \mathcal{E}_4 .

As it seems to be quite hard to compute all D_8 -invariant self-dual overcodes of \mathcal{E}_i for these four codes \mathcal{E}_i we need to apply a different strategy which is based on the fact that $h = (g\sigma)^2$ is the square of an element of order 4. So let

$$k := g\sigma = (1, 8, 3, 6)(2, 5, 4, 7) \dots (66, 69, 68, 71) \in D_8.$$

By [11] we have that \mathcal{C} is a free $\mathbb{F}_2\langle k \rangle$ -module (of rank 9). Since $\langle k \rangle$ is abelian, the module is both left and right; however here we use the right notation. The regular module $\mathbb{F}_2\langle k \rangle$ has a unique irreducible module, 1-dimensional, called the socle, that is $\langle (1 + k + k^2 + k^3) \rangle$. So \mathcal{C} , as a free $\mathbb{F}_2\langle k \rangle$ -module, has socle $\mathcal{C}(k) = \mathcal{C} \cdot (1 + k + k^2 + k^3)$. This implies that, for every basis b_1, \dots, b_9 of $\mathcal{C}(k)$, there exist w_1, \dots, w_9 such that $w_i \cdot (1 + k + k^2 + k^3) = b_i$ and

$$\mathcal{C} = w_1 \cdot \mathbb{F}_2\langle k \rangle \oplus \dots \oplus w_9 \cdot \mathbb{F}_2\langle k \rangle.$$

Then, in order to get all the possible overcodes of \mathcal{E}_i , we choose a basis of the socle $\mathcal{E}_i(k)$, say b_1, \dots, b_9 , and look at the sets

$$W_{i,j} = \{w + \mathcal{E}_i \in \mathcal{E}_i^\perp / \mathcal{E}_i \mid w \cdot (1 + k + k^2 + k^3) = b_j \text{ and } d(\mathcal{E}_i + w \cdot \mathbb{F}_2\langle k \rangle) \geq 16\}$$

For every i we have at least one j for which the set $W_{i,j}$ is empty. This computation hence shows the following main theorem.

Theorem 3.13. The automorphism group of a self-dual $[72, 36, 16]$ code does not contain a subgroup isomorphic to D_8 .

Acknowledgment

The authors like to express their gratitude to A. Previtali for the fruitful discussions in Milan. *Laboratorio di Matematica Industriale e Crittografia* of Trento deserves thanks for the help in the computational part.

References

- [1] C. Aguilar Melchor, P. Gaborit, *On the classification of extremal [36, 18, 8] binary self-dual codes*. IEEE Trans. Inform. Theory 54 (2008) 4743-4750.

- [2] E. F. Assmuss, H.F. Mattson, *New 5-designs*, J. Combin. Theory 6 (1969) 122–151.
- [3] M. Borello, *The automorphism group of a self-dual $[72, 36, 16]$ binary code does not contain elements of order 6*, IEEE Trans. Inform. Theory 58, No. 12 (2012), 7240–7245.
- [4] W. Bosma, J. Cannon, C. Playoust, *The MAGMA algebra system I: The user language*, J. Symbol. Comput. 24 (1997) 235–265.
- [5] S. Bouyuklieva, *On the automorphism group of a doubly even $(72, 36, 16)$ code*, IEEE Trans. Inform. Theory 50 (2004) 544–547.
- [6] S. Bouyuklieva, *On the automorphisms of order 2 with fixed points for the extremal self-dual codes of length $24m$* , Des. Codes Cryptogr. 25 (2002) 5–13.
- [7] L.E. Danielsen, M.G. Parker, *On the Classification of All Self-Dual Additive Codes over $GF(4)$ of length up to 12*, Journal of Combinatorial Theory, Series A 112(7), pp. 1351–1367, October 2006.
- [8] T. Feulner, G. Nebe, *The automorphism group of an extremal $[72, 36, 16]$ code does not contain Z_7 , $Z_3 \times Z_3$, or D_{10}* . IEEE Trans. Inform. Theory 58 (11) 2012, 6916–6924.
- [9] W.C. Huffman, *Automorphisms of codes with application to extremal doubly even codes of length 48*, IEEE Trans. Inform. Theory IT-28 (1982) 511–521.
- [10] C.L. Mallows, N.J.A. Sloane, *An upper bound for self-dual codes*, Information and Control 22 (1973) 188–200.
- [11] G. Nebe, *An extremal $[72, 36, 16]$ binary code has no automorphism group containing $Z_2 \times Z_4$, Q_8 , or Z_{10}* , Finite Fields and their applications 18 (2012) 563–566.
- [12] E.M. Rains, *Shadow bounds for self-dual codes*, IEEE Trans. Inform. Theory 44 (1998), 134–139.
- [13] N.J.A. Sloane, *Is there a $(72; 36)$ $d = 16$ self-dual code?*, IEEE Trans. Inform. Theory 2 (1973) 251.